DETAILED ACTION

1. This is in reply to **REMARKS** filed on 01/27/2010.

2. **Claims 1-12** are pending.

Priority

3. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 10/594,106, filed on 09/25/2006.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William Park, Reg. No. 55,523 on 03/24/2010.

The application has been amended as follows: In the claims,

1. (previously presented) A method for the detection and prevention of intrusions into a computer network with a firewall, the method comprising:

detecting the connections at a central point and before each branch of said network,

selective filtering of the said connections, where said selective filtering stage includes firstly a stage for automatic recognition of the accessing protocol, independently of the communication port used by the said protocol, and secondly, after said accessing protocol has been recognized automatically, a stage for verifying the conformity of each communication flowing in a given connection to the said protocol, to deliver a dynamic authorization for communications resulting from normal operation of the

protocol and to deliver a dynamic rejection for communications resulting from abnormal operation of the protocol,

wherein said check on conformity is performed layer by layer, by successive protocol .analysis of each part of the data packet flowing in the connection corresponding to a given protocol, from the lowest protocol to the highest protocol, and

wherein, since each main connection enabled is able to induce one or more secondary connections, said check on conformity detects the data necessary for opening said secondary connections and dynamically attaches said secondary connections to the authorization for connection of said main connection.

2. (previously presented) A method according to claim 1, wherein, as long as the accessing protocol of a connection is not recognized, the data are accepted but not transmitted.

3. (previously presented) A method according to claim 2, wherein, if the number of data packets accepted but not transmitted exceeds a certain threshold, or if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analyzed.

4. (previously presented) A method according to claim 2, wherein if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analyzed.

5. (previously presented) A method according to claim 2, wherein, when the accessing protocol of a connection is not automatically recognized, said step of- checking on conformity of each communication flowing in a given connection to said protocol is replaced by a step of generic checking of coherence of data packets.

6. (**Currently Amended**) A device for the detection and prevention of intrusions into a computer network, comprising:

a firewall,

a resource for preventing intrusions by detection of the connections, directly incorporated into said firewall at a central point and before each branch of said network, where said resource for the prevention of intrusions includes a resource for selective filtering of said connections by automatic recognition of the accessing protocol, independently of the communication port used by said protocol,

wherein said selective filtering resource includes at least one independent module for the analysis of at least one given communication protocol, and

at least one of the independent modules includes:

i. unit for the automatic recognition of a given communication protocol,

ii. unit for verifying the conformity of the communication flowing in a given connection to the said protocol,

iii. ~~means for~~ **unit for** delivering a dynamic authorization for communications resulting from normal operation of the protocol, and delivering a dynamic rejection for communications resulting from abnormal operation of the protocol, and

iv. ~~means of transmission of a~~ **unit for transmitting** part of a data packet to an independent analysis module of a hierarchically higher protocol, and wherein said unit for verifying the conformity of the communication flowing in a given connection, called main connection, to the said protocol, comprising means of detection of the data necessary for opening secondary connections induced by said main connection, and of attachment of said secondary connections to the authorization for connection of said main connection.

7. (previously presented) A device according to claim 6, wherein, in addition to the independent module or modules for the analysis of a given communication protocol the device includes an independent generic module which attaches itself to the connections for which the protocol has been

recognized by none of the other said independent modules.

8. (previously presented) A device according to claim 6, wherein the device includes an interface for entry, by a user, of the criteria that determine the filtering policy.

9. (previously presented) A device according to claim 8, wherein, said interface receives the criteria specified in natural language by the user.

10. (previously presented) A device according to claim 9, wherein said criteria specified in natural language include at least one protocol name.

11. (previously presented) A device according to claim 8, wherein said interface allows the activation or deactivation of each of said independent modules.

12. (previously presented) A device according to claim 6, wherein the device includes a resource for statistical processing of the connection data, and a resource for storage of said connection data and processed data.

Allowable Subject Matter

5. **Claims 1-12** are allowed in view of amendments and arguments filed on 01/27/2010.

Note: In view of further reading and updated search, and with SPE approval, examiner and applicant's representative agreed to make the examiner's amendment shown above.

By this amendment **Claim 6** is amended.

Contact Information

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **AMARE TABOR** whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Kambiz Zand** can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2434)

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434